

Docket No. YOR919990137US1  
YOR.080

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE  
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re Application of

Andrea CALIFANO, et al.

Serial No.: 09/457,732

Group Art Unit: 2131

Filed: December 10, 1999

Examiner: La Forgia, Christian A.

For: SEMIOTIC SYSTEM AND METHOD WITH PRIVACY PROTECTION

Honorable Commissioner of Patents  
Alexandria, VA 22313-1450

**APPELLANTS' BRIEF ON APPEAL**

Sir:

Appellants respectfully appeal the final rejection of Claims 1, 5-9, and 11-36 in the Office Action dated June 22, 2007. A Notice of Appeal was timely filed on September 24, 2007.

**I. REAL PARTY IN INTEREST**

The real party in interest is International Business Machines Corporation, assignee of 100% interest of the above-referenced patent application.

## **II. RELATED APPEALS AND INTERFERENCES**

There are no other appeals or interferences known to Appellants, Appellants' legal representative or Assignee which would directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

## **III. STATUS OF CLAIMS**

Claims 1, 5-9, and 11-36 are all the claims presently pending in the application, and are set forth fully in the attached Appendix. Claims 1, 5, 9, 15, 17, 19, 24, 27, 29, 31, 33, and 35 are independent claims. Claims 6-8, 11-14, 16, 18, 20-23, 25, 26, 28, 30, 32, 34, and 36 are dependent claims.

### Claims 2-4 and 10 stand canceled.

Claims 1, 14-16, 31, and 32 stand rejected under 35 U.S.C. § 101 as allegedly being inoperative and lacking utility.

Claims 31-36 stand rejected under 35 U.S.C. § 101 as allegedly being directed to non-statutory subject matter.

Claims 1, 5-9, and 11-36 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Borza (U.S. Patent No. 6,446,210) in view of Kharon, et al. (U.S. Patent No. 6,487,662; hereinafter "Kharon").

Appellants' Brief on Appeal  
U.S. Application Serial No. 09/457,732  
Docket No. YOR919990137US1  
(YOR.080)

Appellants respectfully appeal the rejection of Claims 1, 14-16, 31, and 32 under 35 U.S.C. § 101 (utility), the rejection of claims 31-36 under 35 U.S.C. § 101(subject matter), and the rejection of Claims 1, 5-9, and 11-36 under 35 U.S.C. § 103(a) as being unpatentable over Borza in view of Kharon, which are the sole issues in this Appeal.

#### **IV. STATUS OF AMENDMENTS**

A previous Appeal Brief was filed on September 7, 2006. The Examiner issued an Examiner's Answer, which included two new grounds of rejection. The Examiner's Answer, including the new grounds of rejection, was not signed by the Technology Center Director nor the Supervisory Patent Examiner, as required by 37 C.F.R. § 41.39(a)(2) (see also M.P.E.P. § 1207.03).

An Amendment under 37 C.F.R. § 1.111 was filed on January 16, 2007, amending the claims.

The Examiner issued a Final Office Action on June 22, 2007.

An Amendment under 37 C.F.R. § 1.116 was filed on August 22, 2007. The claims were not amended.

A Notice of Appeal was filed timely on September 24, 2007.

Therefore, the claims are pending as set forth in the Appendix, as of the Amendment under 37 C.F.R. § 1.111 filed on January 16, 2007.

## V. SUMMARY OF THE CLAIMED SUBJECT MATTER

With reference to Figures 1-8, the unique and unobvious aspects of the present invention provide a method and system of processing semiotic data that allows use of the data without being a threat to privacy and that prevents misuse of such data, without significantly altering the accuracy and sensitivity of the identification process (e.g., see specification at page 3, lines 9-14).

For example, the claimed invention compares encrypted data against stored encrypted data while at the same time ensuring that unencrypted data is not available or retrievable under the condition that the data might be slightly different from the template. That is, the claimed invention determines whether P is close to P' by comparing only h(P) with h(P'). Thus, in contrast to conventional methods, the claimed invention compares encrypted data against an encrypted template under the possibility that the data might be slightly different from the template (e.g., "close" to the data) (e.g., see specification at page 16, lines 12-17, and pages 17-20).

Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in independent Claim 1) is directed to a method of processing semiotic data (e.g., see Figures 1-4), which includes receiving semiotic data including at least one data set P (e.g., see specification at page 12, lines 4-10, and page 17, line 2-4; see also Figure 1, reference

numeral 101, and Figure 3, reference numeral 301), selecting a function  $h$  (e.g., see specification at page 12, lines 9-10), and for at least one of each the data set  $P$  to be collected, computing  $h(P)$  (e.g., see specification at page 13, lines 3-5; see also Figure 1, reference numeral 102), destroying the data set  $P$  (e.g., see specification at page 13, lines 5-11; see also Figure 1, reference numeral 103), storing  $h(P)$  in a database (e.g., see specification at page 13, line 12; see also Figure 1, reference numeral 104), and obtaining a sample of  $P'$  such that a comparison can be made (e.g., see specification at page 13, lines 18-20; see also Figure 2, reference numeral 201), at least one of obtaining and computing  $h(P')$  (e.g., see specification at page 13, lines 20-21; see also Figure 2, reference numeral 202), and to determine whether  $P'$  is close to a predetermined subject, comparing  $h(P')$  to available  $h(P)$ s to determine whether  $P'$  substantially matches, but does not exactly match, one of the data set  $P$  (e.g., see specification at page 13, lines 13-17, page 14, lines 3-4 and 12-15), wherein the data set  $P$  cannot be extracted from  $h(P)$  (e.g., see specification at page 13, lines 13-14), wherein the semiotic data includes biometric data (e.g., see Figure 1, 101; Figure 2, 201), wherein the function  $h$  includes a secure hash function (e.g., see specification at page 13, lines 3-6), wherein the data set  $P$  is not determined perfectly by its reading (e.g., see specification at page 16, lines 4-8), wherein each reading gives a number  $P_i$  (e.g. see specification at page 16, lines 8-11), wherein  $i$  is no less than 0 (e.g. see specification at page 16, lines 12-14), wherein  $P_0$  is for an initial reading (e.g. see specification at page 16, lines 8-9), and a secret

version of the initial reading is stored after further processing thereof (e.g. see specification at page 16, lines 8-11), wherein reading  $P_0$  is different from  $P_i$  for  $i > 0$  (e.g. see specification at page 16, line 12), and the secret version of  $P_0$  is different from the secret version of  $P_i$  (e.g. see specification at page 16, lines 13-14), such that no identification is possible by a direct comparison of the encrypted data (e.g. see specification at page 16, lines 16-17). The method defined by claim 1, further includes extracting sub-collections  $S_j$  from the collection of data in data set  $P$  (e.g. see specification at page 17, lines 2-6; Figure 3, 302), encrypting a predetermined number of such sub-collections (e.g. see specification at page 17, line 12; Figure 3, 303) such that at least one of the sub-collections is reproduced exactly with a predetermined probability (e.g. see specification at page 17, lines 12-14), comparing (e.g. see specification at page 19, lines 1-4; Figure 4, 405) encrypted versions of the sub-collections  $S_j$  with those data stored in the database (e.g. see specification at page 18, lines 19-20; Figure 3, 305), wherein if one or more of the sub-collection  $S_j$  matches with the data, then verification is deemed to have occurred (e.g. see specification at page 19, lines 3-4), each time a  $P_i$ , with  $i > 0$ , is read, computing all possible predetermined size variations of  $P_i$  which correspond to an acceptable predetermined imprecision of the reading (e.g. see specification at page 19, lines 6-11), and encrypting all such modified data, and comparing the encrypted modified data to data stored in the database (e.g. see specification at page 19, lines 11-12), wherein for a plurality of users of the same biometric information, the biometric

information is encrypted differently for each user (e.g. see specification at page 12, lines 18-20), and wherein at least one of the data set P and P' includes a personal data set (e.g. see specification at page 11, lines 19-22; page 12, line 10; and page 13, lines 20-21).

Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in independent Claim 5) is directed to a method of processing semiotic data (e.g., see Figures 1-4), which includes receiving semiotic data including at least one data set P (e.g., see specification at page 12, lines 4-10, and page 17, line 2-4; see also Figure 1, reference numeral 101, and Figure 3, reference numeral 301), selecting a function h (e.g., see specification at page 12, lines 9-10), and for at least one of each the data set P to be collected, computing h(P) (e.g., see specification at page 13, lines 3-5; see also Figure 1, reference numeral 102), destroying the data set P (e.g., see specification at page 13, lines 5-11; see also Figure 1, reference numeral 103), and storing h(P) in a database (e.g., see specification at page 13, line 12; see also Figure 1, reference numeral 104), wherein the data set P cannot be extracted from h(P) (e.g., see specification at page 13, lines 13-14), the method further includes selecting a private key/public key (K, k) once for all cases (e.g., see specification at page 14, lines 6-7, and one of destroying the private key K and sending the private key K to a trusted party (e.g., see specification at page 14, 7-9), and choosing the function h as the public encryption function corresponding to k (e.g., see specification at page 14, lines 9-11).

According to Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Claim 6) the data set P cannot be extracted from  $h(P)$ , except by the trusted party (e.g., see specification at page 13, lines 13-14; page 14, lines 12-14).

According to Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Claim 7), the method further includes, to determine whether some  $P'$  is a predetermined subject, comparing the  $h(P')$  to available  $h(P)$ s (e.g., see specification at page 14, lines 13-15), and determining whether there is a match (e.g., see specification at page 14, line 15).

According to Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Claim 8) the trusted party includes a panel of members (e.g., see specification at page 14, lines 16-20), and wherein a secret is shared among the members so that only at least a predetermined number of panel members can reconstitute the secret in its entirety by putting together their share of the secret (e.g., see specification at page 14, lines 16-20).

Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Independent Claim 9) is directed to a method of processing semiotic data (e.g., see Figures 1-4), which includes receiving semiotic data including at least one data set P (e.g., see specification at page 12, lines 4-10, and page 17, line 2-4; see also Figure 1, reference numeral 101, and Figure 3, reference numeral 301), selecting a function  $h$  (e.g., see specification at page 12, lines 9-10), and for at least one of each the data set P to be collected,



computing  $h(P)$  (e.g., see specification at page 13, lines 3-5; see also Figure 1, reference numeral 102), destroying the data set  $P$  (e.g., see specification at page 13, lines 5-11; see also Figure 1, reference numeral 103), and storing  $h(P)$  in a database (e.g., see specification at page 13, line 12; see also Figure 1, reference numeral 104), wherein the data set  $P$  cannot be extracted from  $h(P)$  (e.g., see specification at page 13, lines 13-14), wherein the data set  $P$  is not determined perfectly by its reading (e.g., see specification at page 16, lines 4-8), wherein each reading gives a number  $P_i$  (e.g. see specification at page 16, lines 8-11), wherein  $i$  is no less than 0 (e.g. see specification at page 16, lines 12-14), wherein  $P_0$  is for an initial reading (e.g. see specification at page 16, lines 12-14), and a secret version of the initial reading is stored after further processing thereof (e.g. see specification at page 16, lines 8-11), wherein reading  $P_0$  is different from  $P_i$  for  $i > 0$  (e.g. see specification at page 16, line 12), and the secret version of  $P_0$  is different from the secret version of  $P_i$  (e.g. see specification at page 16, lines 13-14), such that no identification is possible by a direct comparison of the encrypted data (e.g. see specification at page 16, lines 16-17). The method defined by claim 9, further includes extracting sub-collections  $S_j$  from the collection of data in data set  $P$  (e.g. see specification at page 17, lines 2-6; Figure 3, 302), encrypting a predetermined number of such sub-collections (e.g. see specification at page 17, line 12; Figure 3, 303) such that at least one of the sub-collections is reproduced exactly with a predetermined probability (e.g. see specification at page 17, lines 12-14).

According to Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Claim 10), the method further includes extracting sub-collections  $S_j$  from the collection of data in data set P (e.g. see specification at page 17, lines 2-6; Figure 3, 302), and encrypting a predetermined number of such sub-collections (e.g. see specification at page 17, line 12; Figure 3, 303) such that at least one of the sub-collections is reproduced exactly with a predetermined probability (e.g. see specification at page 17, lines 12-14).

According to Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Claim 11), the method further includes comparing (e.g. see specification at page 19, lines 1-4; Figure 4, 405) encrypted versions of the sub-collections  $S_j$  with those data stored in the database (e.g. see specification at page 18, lines 19-20; Figure 3, 305), wherein if one or more of the sub-collection  $S_j$  matches with the data, then verification is deemed to have occurred (e.g. see specification at page 19, lines 3-4).

According to Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Claim 12), the method further includes, each time a  $P_i$ , with  $i > 0$ , is read, computing all possible predetermined size variations of  $P_i$  which correspond to an acceptable predetermined imprecision of the reading (e.g. see specification at page 19, lines 6-11), and encrypting all such modified data, and comparing the encrypted modified data to data stored in the database (e.g. see specification at page 19, lines 11-12).

According to Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Claim 13), for a plurality of users of the same biometric information, the biometric information is encrypted differently for each user (e.g. see specification at page 12, lines 18-20).

According to Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Claim 14), at least one of the data set P and P' includes a personal data set (e.g. see specification at page 11, lines 19-22; page 12, line 10; and page 13, lines 20-21).

Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Independent Claim 15), is directed to a method of processing biometric data (e.g., see Figures 1-4), which includes acquiring unencrypted biometric data including at least one data set P (e.g., see specification at page 12, lines 4-10, and page 17, line 2-4; see also Figure 1, reference numeral 101, and Figure 3, reference numeral 301), encrypting, with one of a secure hash function and an identity function, each the at least one data set acquired (e.g., see specification at page 13, lines 3-5; see also Figure 1, reference numeral 102), destroying the unencrypted data set P (e.g., see specification at page 13, lines 5-11; see also Figure 1, reference numeral 103), storing each of the at least one encrypted data set in a database (e.g., see specification at page 13, line 12; see also Figure 1, reference numeral 104), wherein unencrypted biometric data is not available nor retrievable from the data stored in the database (e.g., see specification at page 13, lines 13-14), and to determine whether a data set

P' is a predetermined subject, comparing an encrypted data set of P' to the at least one encrypted data set stored in the database to determine whether the data set P' substantially matches, but does not exactly match, the at least one encrypted data set stored in the database (e.g., see specification at page 13, lines 13-17, page 14, lines 3-4 and 12-15). The method defined by claim 15, further includes extracting sub-collections S<sub>j</sub> from the collection of data in data set P (e.g. see specification at page 17, lines 2-6; Figure 3, 302), encrypting a predetermined number of such sub-collections (e.g. see specification at page 17, line 12; Figure 3, 303) such that at least one of the sub-collections is reproduced exactly with a predetermined probability (e.g. see specification at page 17, lines 12-14), comparing (e.g. see specification at page 19, lines 1-4; Figure 4, 405) encrypted versions of the sub-collections S<sub>j</sub> with those data stored in the database (e.g. see specification at page 18, lines 19-20; Figure 3, 305), wherein if one or more of the sub-collection S<sub>j</sub> matches with the data, then verification is deemed to have occurred (e.g. see specification at page 19, lines 3-4)

According to Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Claim 16), at least one of the data set P and P' includes a personal data set (e.g. see specification at page 11, lines 19-22; page 12, line 10; and page 13, lines 20-21).

Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Independent Claim 17), is directed to a method of extracting components of biometric data which are stable under measurement errors, which includes acquiring unencrypted biometric

data including at least one data set P (e.g., see specification at page 12, lines 4-10, and page 17, line 2-4; see also Figure 1, reference numeral 101, and Figure 3, reference numeral 301), encrypting each the at least one data set acquired to form at least one encrypted data set (e.g., see specification at page 13, lines 3-5; see also Figure 1, reference numeral 102), destroying the unencrypted data set P (e.g., see specification at page 13, lines 5-11; see also Figure 1, reference numeral 103), storing each the at least one encrypted data set in a database (e.g., see specification at page 13, line 12; see also Figure 1, reference numeral 104), wherein unencrypted biometric data is not available nor retrievable from the data stored in the database (e.g., see specification at page 13, lines 13-14), and to determine whether a data set P' is a predetermined subject, comparing an encrypted data set of P' to the at least one encrypted data set stored in the database to determine whether there is a match (e.g., see specification at page 13, lines 13-17, page 14, lines 3-4 and 12-15). The method defined by claim 17, further includes extracting sub-collections S<sub>j</sub> from the collection of data in data set P (e.g. see specification at page 17, lines 2-6; Figure 3, 302), encrypting a predetermined number of such sub-collections (e.g. see specification at page 17, line 12; Figure 3, 303) such that at least one of the sub-collections is reproduced exactly with a predetermined probability (e.g. see specification at page 17, lines 12-14), comparing (e.g. see specification at page 19, lines 1-4; Figure 4, 405) encrypted versions of the sub-collections S<sub>j</sub> with those data stored in the database (e.g. see specification at page 18, lines 19-20; Figure 3, 305), wherein if one or

more of the sub-collection  $S_j$  matches with the data, then verification is deemed to have occurred (e.g. see specification at page 19, lines 3-4).

According to Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Claim 18), at least one of the data set  $P$  and  $P'$  includes a personal data set (e.g. see specification at page 11, lines 19-22; page 12, line 10; and page 13, lines 20-21).

Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Independent Claim 19), is directed to a method of extracting components of biometric data which are stable under measurement errors, includes acquiring unencrypted biometric data including at least one data set  $P$  (e.g., see specification at page 12, lines 4-10, and page 17, line 2-4; see also Figure 1, reference numeral 101, and Figure 3, reference numeral 301), encrypting each the at least one data set acquired to form at least one encrypted data set (e.g., see specification at page 13, lines 3-5; see also Figure 1, reference numeral 102), destroying the unencrypted data set  $P$  (e.g., see specification at page 13, lines 5-11; see also Figure 1, reference numeral 103), and storing each the at least one encrypted data set in a database (e.g., see specification at page 13, line 12; see also Figure 1, reference numeral 104), wherein unencrypted biometric data is not available nor retrievable from the data stored in the database (e.g., see specification at page 13, lines 13-14), extracting sub-collections  $S_j$  from the collection of data in the data set  $P$  (e.g. see specification at page 17, lines 2-6; Figure 3, 302), and encrypting a predetermined number of such sub-collections (e.g. see specification

at page 17, line 12; Figure 3, 303) such that at least one of the sub-collections is reproduced exactly with a predetermined probability (e.g. see specification at page 17, lines 12-14).

According to Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Claim 20), the data set includes a personal data set (e.g. see specification at page 11, lines 19-22; page 12, line 10; and page 13, lines 20-21).

According to Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Claim 21), the method further includes comparing encrypted versions of the sub-collections  $S_j$  with those data stored in the database (e.g. see specification at page 17, lines 2-6; Figure 3, 302), wherein if one or more of the sub-collection  $S_j$  matches with the data, then verification is deemed to have occurred (e.g. see specification at page 19, lines 3-4).

According to Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Claim 22), a data set  $P$  is not determined perfectly by its reading (e.g., see specification at page 16, lines 4-8), such that each reading gives a number  $P_i$  (e.g., see specification at page 16, lines 4-8), wherein  $i$  is no less than 0 (e.g. see specification at page 16, lines 12-14), wherein  $P_0$  is for an initial reading (e.g. see specification at page 16, lines 8-9), and a secret version of the initial reading is stored after further processing thereof (e.g. see specification at page 16, lines 8-11), wherein reading  $P_0$  is different from  $P_i$  for  $i > 0$  (e.g. see specification at page 16, line 12), and the secret version of  $P_0$  is different from the secret version of  $P_i$  (e.g. see specification at page 16, lines 13-14), such that no identification

is possible by a direct comparison of the encrypted data (e.g. see specification at page 16, lines 16-17).

According to Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Claim 23), the method further includes each time a data set is read  $P_i$ , with  $i > 0$ , is read, computing all possible predetermined size variations of  $P_i$  which correspond to an acceptable predetermined imprecision of the reading (e.g. see specification at page 19, lines 6-11), and encrypting all such modified data, and comparing the encrypted modified data to data stored in the database (e.g. see specification at page 19, lines 11-12).

Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Independent Claim 24), is directed to a system for processing semiotic data, which includes means for receiving semiotic data including a data set  $P$  (e.g., see specification at page 12, lines 4-10, and page 17, line 2-4; see also Figure 1, reference numeral 101, Figure 3, reference numeral 301, Figure 7, reference numeral 718), means for selecting a function  $h$ , and for each the data set  $P$  to be collected, computing  $h(P)$  (e.g., see specification at page 13, lines 3-5; see also Figure 1, reference numeral 102; Figure 7, 711), means for destroying the data set  $P$  (e.g., see specification at page 13, lines 5-11; see also Figure 1, reference numeral 103; Figure 7, 711), means for storing  $h(P)$  in a database (e.g., see specification at page 13, line 12; see also Figure 1, reference numeral 104; Figure 7, 718), wherein the data set  $P$  cannot be extracted from  $h(P)$  (e.g., see specification at page 13, lines 13-14), and to



determine whether a data set P' is close to a predetermined subject, means for comparing  $h(P')$  to available  $h(P)$ s to determine whether data set P' is close to some P (e.g., see specification at page 13, lines 13-17, page 14, lines 3-4 and 12-15; see Figure 7, 711).

According to Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Claim 25), the semiotic data includes biometric data (e.g., see Figure 1, 101; Figure 2, 201).

According to Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Claim 26), at least one of the data set P and P' includes a personal data set (e.g. see specification at page 11, lines 19-22; page 12, line 10; and page 13, lines 20-21).

Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Independent Claim 27), is directed to a system for verifying biometric data without storing unencrypted biometric data, includes means for acquiring unencrypted biometric data including at least one data set P (e.g., see specification at page 12, lines 4-10, and page 17, line 2-4; see also Figure 1, reference numeral 101, Figure 3, reference numeral 301; Figure 7, 718), means for encrypting each the at least one data set acquired to form at least one encrypted data set (e.g., see specification at page 13, lines 3-5; see also Figure 1, reference numeral 102; Figure 7, 711), means for destroying the unencrypted data set P (e.g., see specification at page 13, lines 5-11; see also Figure 1, reference numeral 103; Figure 7, 711), means for storing each the at least one encrypted data set in a database (e.g., see specification

at page 13, line 12; see also Figure 1, reference numeral 104; Figure 7, 718), wherein unencrypted biometric data is not available nor retrievable from the data stored in the database (e.g., see specification at page 13, lines 13-14), and means for comparing an encrypted data set of a data set P' to the at least one encrypted data set of data set P to determine whether there is a match and to determine whether the data set P' is a predetermined subject (e.g., see specification at page 13, lines 13-17, page 14, lines 3-4 and 12-15; See Figure 7, 711).

According to Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Claim 28), at least one of the data set P and P' includes a personal data set (e.g. see specification at page 11, lines 19-22; page 12, line 10; and page 13, lines 20-21).

Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Independent Claim 29), is directed to a system (e.g., see Figure 7) for extracting components of biometric data which are stable under measurement errors, includes acquiring unencrypted biometric data including at least one data set P (e.g., see specification at page 12, lines 4-10, and page 17, line 2-4; see also Figure 1, reference numeral 101, and Figure 3, reference numeral 301), encrypting each the at least one data set acquired to form at least one encrypted data set (e.g., see specification at page 13, lines 3-5; see also Figure 1, reference numeral 102), destroying the unencrypted data set P (e.g., see specification at page 13, lines 5-11; see also Figure 1, reference numeral 103), and storing each the at least one encrypted

data set in a database (e.g., see specification at page 13, line 12; see also Figure 1, reference numeral 104), wherein unencrypted biometric data is not available nor retrievable from the data stored in the database (e.g., see specification at page 13, lines 13-14), extracting sub-collections  $S_j$  from the collection of data in the data set P (e.g. see specification at page 17, lines 2-6; Figure 3, 302), and encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability.

According to Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Claim 30), the data set includes a personal data set (e.g. see specification at page 11, lines 19-22; page 12, line 10; and page 13, lines 20-21).

Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Independent Claim 31) is directed to a computer-readable medium tangibly embodying a program of recordable, machine-readable instructions executable by a digital processing apparatus to perform a method for computer-implemented processing biometric data, in which the method includes receiving biometric data including a data set P (e.g., see specification at page 12, lines 4-10, and page 17, line 2-4; see also Figure 1, reference numeral 101, and Figure 3, reference numeral 301), selecting a secure hash function  $h$ , and for each data set P to be collected, computing  $h(P)$  (e.g., see specification at page 13, lines 3-5; see also Figure 1, reference numeral 102), destroying the data set P (e.g., see specification

at page 13, lines 5-11; see also Figure 1, reference numeral 103), storing  $h(P)$  in a database (e.g., see specification at page 13, line 12; see also Figure 1, reference numeral 104), wherein the data set  $P$  cannot be extracted from  $h(P)$  (e.g., see specification at page 13, lines 13-14), and to determine whether a data set  $P'$  is close to a predetermined subject, comparing  $h(P')$  to available  $h(P)$ s to determine whether data set  $P'$  is close to some data set  $P$ .

According to Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Claim 32), at least one of the data set  $P$  and  $P'$  includes a personal data set (e.g. see specification at page 11, lines 19-22; page 12, line 10; and page 13, lines 20-21).

Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Independent Claim 33), is directed to a computer-readable medium tangibly embodying a program of recordable, machine-readable instructions executable by a digital processing apparatus to perform a method for computer-implemented verifying of biometric data without storing unencrypted biometric data, the method includes acquiring unencrypted biometric data including at least one data set  $P$  (e.g., see specification at page 12, lines 4-10, and page 17, line 2-4; see also Figure 1, reference numeral 101, and Figure 3, reference numeral 301), encrypting each the at least one data set acquired to form at least one encrypted data set (e.g., see specification at page 13, lines 3-5; see also Figure 1, reference numeral 102), destroying the unencrypted data set  $P$  (e.g., see specification at page 13, lines 5-11; see also Figure 1, reference numeral 103), storing each the at least one encrypted data

set in a database (e.g., see specification at page 13, line 12; see also Figure 1, reference numeral 104), wherein unencrypted biometric data is not available nor retrievable from the data stored in the database (e.g., see specification at page 13, lines 13-14), and to determine whether a data set P' is close to a predetermined subject, comparing an encrypted data set of P' to the at least one encrypted data set to determine whether data set P' is close to some data set P. The method defined by claim 33, further includes extracting sub-collections S<sub>j</sub> from the collection of data in data set P (e.g. see specification at page 17, lines 2-6; Figure 3, 302), encrypting a predetermined number of such sub-collections (e.g. see specification at page 17, line 12; Figure 3, 303) such that at least one of the sub-collections is reproduced exactly with a predetermined probability (e.g. see specification at page 17, lines 12-14), comparing (e.g. see specification at page 19, lines 1-4; Figure 4, 405) encrypted versions of the sub-collections S<sub>j</sub> with those data stored in the database (e.g. see specification at page 18, lines 19-20; Figure 3, 305), wherein if one or more of the sub-collection S<sub>j</sub> matches with the data, then verification is deemed to have occurred (e.g. see specification at page 19, lines 3-4).

According to Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Claim 34), at least one of the data set P and P' includes a personal data set.

Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Independent Claim 35) is directed to a computer-readable medium tangibly embodying a program of recordable, machine-readable instructions executable by a digital processing

apparatus to perform a method for computer-implemented extracting components of biometric data which are stable under measurement errors, the method includes acquiring unencrypted biometric data including at least one data set P (e.g., see specification at page 12, lines 4-10, and page 17, line 2-4; see also Figure 1, reference numeral 101, and Figure 3, reference numeral 301), encrypting each the at least one data set acquired to form at least one encrypted data set (e.g., see specification at page 13, lines 3-5; see also Figure 1, reference numeral 102), destroying the unencrypted data set P (e.g., see specification at page 13, lines 5-11; see also Figure 1, reference numeral 103), storing each the at least one encrypted data set in a database (e.g., see specification at page 13, line 12; see also Figure 1, reference numeral 104), wherein unencrypted biometric data is not available nor retrievable from the data stored in the database (e.g., see specification at page 13, lines 13-14), extracting sub-collections  $S_j$  from the collection of data in the data set P (e.g. see specification at page 17, lines 2-6; Figure 3, 302), and encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability.

According to Appellants' invention, as disclosed and claimed (e.g., as exemplarily defined in Claim 36), the data set includes a personal data set (e.g. see specification at page 11, lines 19-22; page 12, line 10; and page 13, lines 20-21).

## **VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL**

The issues presented for review by the Board of Patent Appeals and Interferences are whether Claims 1, 14-16, 31, and 32 stand rejected under 35 U.S.C. § 101 for lack of utility, Claims 31-36 stand rejected under 35 U.S.C. § 101 for being directed to non-statutory subject matter, and Claims 1 and 5-36 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Borza in view of Kharon.

## **VII. ARGUMENT**

### **A. THE EXAMINER'S POSITION**

In the Advisory Action mailed August 29, 2007, the Examiner stated that the Amendment under 37 C.F.R. § 1.116 had been considered (see Advisory Action at paragraph 11), but held Claims 1, 5-9, and 11-36 unpatentable for the reasons previously identified in the final Office Action (see Advisory Action at Continuation of 11).

The Examiner maintained that Claims 1, 14-16, 31, and 32 stand rejected under 35 U.S.C. § 101, that Claims 31-36 stand rejected under 35 U.S.C. § 101, and that Claims 1 and 5-36 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Borza in view of Kharon.

**B. APPELLANTS' POSITION**

For at least the foregoing reasons, Appellants respectfully disagree with the Examiner's positions, and therefore, Appellants traverse each of the Examiner's rejections.

**1. REJECTION UNDER 35 U.S.C. § 101 (Alleged Lack of Utility)**

Claims 1, 14-16, 31, and 32 stand rejected under 35 U.S.C. § 101 as allegedly being inoperative and lacking utility. That is, the Examiner asserts that the claimed invention "*could not work*", as evidenced by the Handbook of Applied Cryptography.

Appellants respectfully disagree with each of the Examiner's positions, for the following reasons.

Appellants respectfully submit that the Examiner is misunderstanding the invention and Appellants' traversal arguments. Moreover, the Examiner has misapplied the teachings of the Handbook of Applied Cryptography, in view of this apparent misunderstanding of Appellants' traversal position.

Appellants submit that the disclosure of the present application explicitly acknowledges the problem that a simple hash function approach would not work (as disclosed in the above Handbook and as suggested by the Examiner in the March 7, 2006 Office Action at page 4, numbered paragraph 11)(e.g., see specification at page 16, lines 15-17).



Specifically, the specification of the present application (at page 16, lines 15-17) states that:

Because  $P0$  is in general (possibly) slightly different form  $Pi$  for  $i > 0$ , the secret version of  $p0$  will generally be quite different from the secret version of  $Pi$ . This is because cryptographic functions are extremely sensitive to the input, thereby to be resilient to attempts to decode the encrypted data. In this case, no identification is possible by direct comparison of the encrypted data (emphasis added).

Accordingly, the present application discloses several approaches to compare encrypted or hashed data under uncertainty (e.g., see specification at page 16, line 18 to page 20, line 8).

That is, the specification specifically describes three basis methods to circumvent the above situation and the sensitivity of the cryptographic functions (e.g., see specification at page 16, lines 18-19). Indeed, pages 17-20 of the specification specifically describe a first exemplary method, a second exemplary method, and a third exemplary method for circumventing the very problem with comparing encrypted or hash data, which the Examiner mentions in the Office Action.

Thus, the Examiner's continued assertion that the invention is inoperable because of the teachings of the Handbook of Applied Cryptography and section 9.2.2 Basis Properties and Definitions clearly is erroneous, as a matter of both fact and law. That is, the Examiner has failed to consider the specific disclosure of the present application, which clearly

describes a novel **solution for circumventing the problem** being relied upon by the Examiner in the Handbook of Applied Cryptography.

Indeed, the disclosure of the present application clearly does not contradict the teachings of the Handbook of Applied Cryptography, upon which the Examiner relies.

Instead, the present invention clearly explains a method of **circumventing** the very problems which the Handbook of Applied Cryptography identifies and for which the Handbook is being relied upon by the Examiner as teaching.

Indeed, the Examiner has erroneously interpreted what the invention teaches in a way that clearly does not comport with the actual disclosure of the present application.

For example, in paragraph 11 of the March 7, 2006 Office Action, the Examiner states that the claims “*generally relate to ...*”. Thus, the Examiner appears to have improperly attempted to distill the invention down to a gist of the invention.

However, the Examiner's position clearly fails to consider all of the teachings of the invention (i.e., the actual disclosure of the present application), or for that matter, the specific features recited in the claims.

As Appellants have explained in each of the previous Amendments, the claimed invention compares encrypted data against stored encrypted data while at the same time ensuring that unencrypted data is not available or retrievable under the condition that the data might be slightly different from the template. That is, the claimed invention determines

whether P is close to P' by comparing only h(P) with h(P') (e.g., see specification at page 16, lines 12-17, and pages 17-20).

(The traversal arguments set forth in the Amendment under 37 C.F.R. § 1.111 filed on June 18, 2004, the Amendment under 37 C.F.R. § 1.116 filed on January 18, 2005, the Amendment under 37 C.F.R. § 1.111 filed on April 15, 2005, the Amendment under 37 C.F.R. § 1.116 filed on July 11, 2005, the Amendment under 37 C.F.R. § 1.111 filed on December 16, 2005, the Amendment under 37 C.F.R. § 1.111 filed on January 16, 2007, and the Amendment 37 C.F.R. § 1.116 filed on August 22, 2007 are incorporated herein by reference in their entirety.)

Thus, the present application explains that, in contrast to conventional methods, the claimed invention compares encrypted data against an encrypted template under the possibility that the data might be slightly different from the template (e.g., “close” to the data) (e.g., see specification at page 16, lines 12-17, and pages 17-20).

Indeed, the claimed invention does not merely “generally relate to comparing two separate, imperfect samples of biometric data using a hash function to provide authentication”, as alleged by the Examiner.

That is, the claimed invention does NOT use a hash function by ITSELF to authenticate two samples, as erroneously alleged by the Examiner. Instead, a hash function

is only part of the novel solution provided by the present invention for circumventing the identified problems with the prior art.

Moreover, not all of the claims deal with imperfect biometric data. Instead, only some of the claims deal with such imperfect data.

For the foregoing reasons, Appellants respectfully submit that the claimed invention could (and does) work for its intended purpose, as disclosed in the disclosure of the present application (e.g., see specification at page 16, lines 12-17, and page 17, line 1, to page 20, line 8).

Moreover, the present application specifically states that the claimed invention provides a method and system of processing semiotic data that allows use of the data without being a threat to privacy and that prevents misuse of such data, without significantly altering the accuracy and sensitivity of the identification process (e.g., see specification at page 3, lines 9-14).

The specification specifically discloses comparing encrypted data against stored encrypted data while at the same time ensuring that unencrypted data is not available or retrievable under the condition that the data might be slightly different from the template. That is, the claimed invention determines whether P is close to P' by comparing only h(P) with h(P'). The specification states that, in contrast to conventional methods, the claimed invention compares encrypted data against an encrypted template under the possibility that

the data might be slightly different from the template (e.g., "close" to the data) (e.g., see specification at page 16, lines 12-17, and pages 17-20).

Thus, contrary to the Examiner's position, Appellants respectfully submit that claims 1, 14-16, 31, and 32:

(1) are supported by a specific and substantial asserted utility or a well established utility,

(2) are not inoperative and do not lack utility, and

(3) could (and do) work for their intended purpose, as disclosed in the disclosure of the specification of the present application, for example, at page 16, lines 12-17, and page 17, line 1, to page 20, line 8.

The Examiner has not explained why the Examiner doubts the truth or veracity of Appellants' disclosure.

Moreover, In the Response to Arguments of the Examiner's Answer (dated November 13, 2006), the Examiner stated that:

In response to the Appellant's position that the Examiner did not respond to or answer the substance of the Appellant's traversal, the Examiner disagrees. In response to a proper 35 U.S.C. 101 rejection, the burden shifts to the appellant to rebut the prima facie showing. The Appellant may rebut this rejection using any combination of the following: amendments to the claims, arguments or reasoning, or new evidence submitted in an affidavit or declaration under 37 CFR 1.132, or in a printed publication.

(see Examiner's Answer at page 13; emphasis added Applicants).

In the Response to Arguments, the Examiner further stated that:

In response to the requirement, the Appellant did not amend the claims, submit an affidavit or declaration, or a printed publication to rebut the Examiner's rejection. Instead the Appellant chose to argue by referring back to the specification of the instant application and arguing that the hashes produced are close. The Appellant is reminded that the features upon which appellant relies, such as the methods disclosed in the specification, are not recited in the rejected claims. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). The Examiner has considered the specification, claims, and prior art before making the rejection and believes the asserted utility would be incredible to a person of ordinary skill in the art. See *In re Rinehart*, 531 F.2d 1048, 1052, 189 USPQ 143, 147 (CCPA 1976).

(see Examiner's Answer at page 13; emphasis added Applicants).

Next, in the Response to Arguments, the Examiner stated that:

The Appellant failed to properly address the Examiner's *prima facie* showing of the inoperability of the instant invention and the Examiner responded in the only method available at the time, and as such the rejection should be maintained.

(see Examiner's Answer at page 13; emphasis added Applicants).

Appellants respectfully disagree.

Appellants submit that, as the Examiner acknowledged, Appellants may rebut the rejection using any combination of amendments to the claims, arguments or reasoning, or new evidence submitted in an affidavit or declaration under 37 CFR 1.132, or in a printed publication. Next, the Examiner acknowledged that "the Appellant chose to argue by referring back to the specification of the instant application and arguing that the hashes produced are close" (see Examiner's Answer

Appellants' Brief on Appeal  
U.S. Application Serial No. 09/457,732  
Docket No. YOR919990137US1  
(YOR.080)

at page 13; emphasis added Appellants).

Thus, it is unclear to Appellants how the Examiner then takes the position that "Appellant failed to properly address the Examiner's *prima facie* showing of the inoperability of the instant invention". Indeed, the Examiner's statement seems to be contrary to the previous statements, which indicate that Applicants did address the Examiner's alleged *prima facie* case.

Turning again to the Response to Arguments in the Examiner's Answer, the Examiner states that:

In response to the Appellant's arguments that the Examiner is not considering the Appellant's actual argument or the actual disclosure of the invention, the Examiner disagrees. The Appellant agrees with the Examiner's position that a simple hash function would not work on page 26 of the Appeal Brief filed 07 September 2006. The Appellant refers to methods for circumventing the problems of comparing encrypted or hashed data samples **but is reminded that the features upon which appellant relies are not recited in the rejected claims**. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

(see Examiner's Answer at page 14, last paragraph; emphasis added Applicants).

Appellants respectfully disagree.

Contrary to the Examiner's position, Appellants respectfully submit that the features upon which Appellants rely clearly are recited in the rejected claims.

**Independent claim 1**

For example, turning to the specific language of independent claim 1, the claimed invention recites a method of processing semiotic data, including:

*receiving semiotic data including at least one data set P;  
selecting a function h, and for at least one of each said data set P to be collected, computing h(P);  
destroying said data set P;  
storing h(P) in a database, and  
obtaining a sample of P' such that a comparison can be made;  
at least one of obtaining and computing h(P'); and  
**to determine whether P' is close to a predetermined subject, comparing h(P') to available h(P)s to determine whether P' substantially matches, but does not exactly match, one of said data set P,**  
wherein said data set P cannot be extracted from h(P),  
wherein said semiotic data comprises biometric data,  
wherein said function h comprises a secure hash function,  
wherein the data set P is not determined perfectly by its reading,  
wherein each reading gives a number  $P_i$ , wherein i is no less than 0,  
wherein  $P_0$  is for an initial reading, and a secret version of said initial reading is stored after further processing thereof,  
wherein reading  $P_0$  is different from  $P_i$  for  $i > 0$ , and the secret version of  $P_0$  is different from the secret version of  $P_i$ , such that no identification is possible by a direct comparison of the encrypted data,  
said method further comprising:  
**extracting sub-collections  $S_j$  from the collection of data in data set P;**  
**encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability,**  
**comparing encrypted versions of the sub-collections  $S_j$  with those data stored in said database,**  
**wherein if one or more of the sub-collection  $S_j$  matches with said data, then verification is deemed to have occurred,***



*each time a  $P_i$ , with  $i > 0$ , is read, computing all possible predetermined size variations of  $P_i$  which correspond to an acceptable predetermined imprecision of the reading; and  
encrypting all such modified data, and comparing said encrypted modified data to data stored in said database,  
wherein for a plurality of users of the same biometric information, said biometric information is encrypted differently for each user, and  
wherein at least one of said data set  $P$  and  $P'$  comprises a personal data set (emphasis added Applicants).*

Thus, independent claim 1 clearly defines a method in which, “to determine whether  $P'$  is close to a predetermined subject, comparing  $h(P')$  to available  $h(P)$ s to determine whether  $P'$  substantially matches, but does not exactly match, one of said data set  $P$ ” (emphasis added Applicants). Independent claims 15 and 32 recite somewhat similar features.

Moreover, independent claim 1 further recites “extracting sub-collections  $S_j$  from the collection of data in data set  $P$ ; encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability, comparing encrypted versions of the sub-collections  $S_j$  with those data stored in said database, wherein if one or more of the sub-collection  $S_j$  matches with said data, then verification is deemed to have occurred” (emphasis added Appellants).

Contrary to the Examiner's position, Appellants submit that the features which are described at pages 17-20 of the present application are, in fact, recited by independent claim 1.

For the foregoing reasons, Applicants respectfully reiterate that the claimed invention could (and does) work for its intended purpose, as disclosed in the disclosure of the present application (e.g., see specification at page 16, lines 12-17, and page 17, line 1, to page 20, line 8).

Moreover, the present application specifically states that the claimed invention provides a method and system of processing semiotic data that allows use of the data without being a threat to privacy and that prevents misuse of such data, without significantly altering the accuracy and sensitivity of the identification process (e.g., see specification at page 3, lines 9-14).

The specification specifically discloses comparing encrypted data against stored encrypted data while at the same time ensuring that unencrypted data is not available or retrievable under the condition that the data might be slightly different from the template. That is, the claimed invention determines whether P is close to P' by comparing only h(P) with h(P'). The specification states that, in contrast to conventional methods, the claimed invention compares encrypted data against an encrypted template under the possibility that the data might be slightly different from the template (e.g., “close” to the data) (e.g., see specification at page 16, lines 12-17, and pages 17-20).

Thus, contrary to the Examiner's position, Appellants respectfully reiterate that claims 1, 14-16, 31, and 32:

- (1) are supported by a specific and substantial asserted utility or a well established utility,
- (2) are not inoperative and do not lack utility, and
- (3) could (and do) work for their intended purpose,

as disclosed in the disclosure of the specification of the present application, for example, at page 3, lines 9-14, page 16, lines 12-17, and page 17, line 1, to page 20, line 8.

Appellants reiterate that, to date, the Examiner has not explained why the Examiner doubts the truth or veracity of Appellants' disclosure, or provided any reasons as to why the actual disclosure of the present application would be inoperative and lack utility.

Turning again to the Response to Arguments in the Examiner's Answer, the Examiner states that:

The Examiner would like to point out that the **Appellant fails to define/redefine the term hash function to coincide with a particular method disclosed in the specification.** Where appellant acts as his or her own lexicographer to specifically define a term of a claim contrary to its ordinary meaning, the written description must clearly redefine the claim term and set forth the uncommon definition so as to put one reasonably skilled in the art on notice that the appellant intended to so redefine that claim term. *Process Control Corp. v. HydReclaim Corp.*, 190 F.3d 1350, 1357, 52 USPQ2d 1029, 1033 (Fed. Cir. 1999). The Appellant has not elaborated in the claim language that the hash function is one of the disclosed methods on pages 17-20 of the specification. The Appellant fails to meet the requirements of redefining a term as set forth in the MPEP § 2106. In order to define/redefine a term, the Appellant must do so "with reasonable clarity, deliberateness, and precision" and must "set out his uncommon definition in some manner within the patent disclosure" so as to give one of ordinary skill in the art notice of the change" in meaning.

(see Examiner's Answer at page 14, last paragraph; emphasis added Applicants).

Contrary to the Examiner's position, Appellants submit that nowhere in the present

application, or in the previous Responses, have Appellants attempted to define or redefine the term “*hash function*”, or be their own lexicographer of the term “*hash function*”, or for that matter, assert that the claimed term “*hash function*”, by itself, is defined as “one of the disclosed methods on pages 17-20 of the specification” (see Examiner’s Answer at page 14, last paragraph).

Instead, Appellants argued that the Examiner was misunderstanding the invention and Applicants’ traversal arguments. Moreover, Appellants argued that the Examiner had misapplied the teachings of the Handbook of Applied Cryptography, in view of this apparent misunderstanding of Applicants’ traversal position.

Moreover, as mentioned above, Appellants argued, *inter alia*, that the present application discloses several approaches to compare encrypted or hashed data under uncertainty (e.g., see specification at page 16, line 18 to page 20, line 8). That is, the specification specifically describes three basis methods to circumvent the above situation and the sensitivity of the cryptographic functions (e.g., see specification at page 16, lines 18-19). Indeed, pages 17-20 of the specification specifically describe a first exemplary method, a second exemplary method, and a third exemplary method for circumventing the very problem with comparing encrypted or hash data.

Thus, Appellants argued that the Examiner’s continued assertion that the invention is inoperable because of the teachings of the Handbook of Applied Cryptography and section

9.2.2 Basis Properties and Definitions clearly was erroneous, as a matter of both fact and law. That is, the Examiner had failed to consider the specific disclosure of the present application, which clearly describes a novel **solution for circumventing the problem being relied upon by the Examiner in the Handbook of Applied Cryptography**. Indeed, the disclosure of the present application clearly does not contradict the teachings of the Handbook of Applied Cryptography, upon which the Examiner relies.

Instead, the present invention clearly explains a method of **circumventing** the very problems which the Handbook of Applied Cryptography identifies and for which the Handbook is being relied upon by the Examiner as teaching.

As Applicants have explained in each of the previous Amendments and the previous Appeal Brief, the claimed invention compares encrypted data against stored encrypted data under the condition that the data might be slightly different from the template. That is, the claimed invention determines whether P is close to P' by comparing only h(P) with h(P') (e.g., see specification at page 16, lines 12-17, and pages 17-20).

Thus, the present application explains that, in contrast to conventional methods, the claimed invention compares encrypted data against an encrypted template under the possibility that the data might be slightly different from the template (e.g., "close" to the data) (e.g., see specification at page 16, lines 12-17, and pages 17-20).

That is, the claimed invention does NOT use a hash function by ITSELF to

authenticate two samples, as erroneously alleged by the Examiner. Instead, a hash function is only part of the novel solution provided by the present invention for circumventing the identified problems with the prior art.

Thus, it is unclear how the Examiner's Response to Arguments, or the cited case law with respect to defining claim terms, is germane to this rejection.

Next, in the Response to Arguments, the Examiner stated that:

The Examiner has considered the claim language as a whole and in light of the specification, and has refrained from reading limitations from the specification into the claim language, especially giving the "hash function" its broadest reasonable interpretation. The Examiner does not disagree with the Appellant that the disclosure of the invention is operable, but the claim language as broadly interpreted by the Examiner provides for an inoperable invention and the rejection should be maintained.

(see Examiner's Answer at page 14; emphasis added Applicants).

Applicants respectfully submit that the Examiner's position is not understood.

First, as set forth in M.P.E.P. § 2111, during patent examination, the pending claims must be "given their broadest reasonable interpretation consistent with the specification." (emphasis added Applicants). The Federal Circuit's *en banc* decision in Phillips v. AWH Corp., 415 F.3d 1303, 75 USPQ2d 1321 (Fed. Cir. 2005) expressly recognized that the USPTO employs the "broadest reasonable interpretation" standard:

The Patent and Trademark Office ("PTO") determines the scope of claims in patent applications not solely on the basis of the claim language, but upon giving claims their broadest reasonable construction "in light of the specification as it

would be interpreted by one of ordinary skill in the art." In re Am. Acad. of Sci. Tech. Ctr., 367 F.3d 1359, 1364[, 70 USPQ2d 1827] (Fed. Cir. 2004). Indeed, the rules of the PTO require that application claims must "conform to the invention as set forth in the remainder of the specification and the terms and phrases used in the claims must find clear support or antecedent basis in the description so that the meaning of the terms in the claims may be ascertainable by reference to the description." 37 CFR 1.75(d)(1). 415 F.3d at 1316, 75 USPQ2d at 1329.

Appellants also note that "reading a claim in light of the specification, to thereby interpret limitations explicitly recited in the claim, is a quite different thing from 'reading limitations of the specification into a claim,' to thereby narrow the scope of the claim by implicitly adding disclosed limitations which have no express basis in the claim." See In re Prater, 415 F.2d 1393, 1404-05, 162 USPQ 541, 550-51 (CCPA 1969)

In this case, Appellants submit that the Examiner's broad interpretation is not a reasonable interpretation, in view of the specification.

That is, the Examiner specifically concedes that "the disclosure of the invention is operable". Thus, it is unclear how the explicitly recited features of independent claims 1, 15, and 32, which clearly recite a method in which, "*to determine whether P' is close to a predetermined subject, comparing h(P') to available h(P)s to determine whether P' substantially matches, but does not exactly match, one of said data set P"*, and which correspond to the features of the invention described, for example, at pages 17-20, could reasonably be interpreted to not be operable when interpreted in light of the specification.

Moreover, if, as the Examiner concedes, “the disclosure of the invention is operable”, then it is unclear how the explicitly recited features of independent claim 1, which further recites a method including extracting sub-collections  $S_j$  from the collection of data in data set  $P$ ; encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability, comparing encrypted versions of the sub-collections  $S_j$  with those data stored in said database, wherein if one or more of the sub-collection  $S_j$  matches with said data, then verification is deemed to have occurred” (emphasis added Applicants), would not be operable when reasonably interpreted in light of the specification.

Again, the Examiner concedes that “the disclosure of the invention is operable”.

However, the Examiner has not identified or establish what information allegedly is missing from the claims (e.g., independent claim 1), which would result in such a broad interpretation of the claims that renders independent claim 1 inoperable in view of the operable disclosure.

Appellants submit that interpreting the explicitly recited features of the claims in a manner that would render the claims inoperable, and thus, in manner that is broader than the actual disclosure of the application, would not be a reasonably broad interpretation, particularly, since the actual disclosure is conceded to be operable (e.g., see specification at pages 17-20).



That is, Appellants submit that it would not be reasonable to interpret the above-identified recitations of independent claim 1 so broadly that they are rendered inoperable, despite the features of the disclosure which are conceded to be operable.

On the contrary, Appellants submit that the ordinarily skilled artisan reasonably would consider the explicitly recited features of the claims to be operable in view of the operable disclosure (e.g., see specification at pages 17-20).

Moreover, in the Response to Arguments of the Final Office Action dated June 22, 2007, The Examiner alleges, "the Applicant fails to define/redefine the term hash function to coincide with a particular method disclosed in the specification. Where applicant acts as his or her own lexicographer to specifically define a term of a claim contrary to its ordinary meaning, the written description must clearly redefine the claim term and set forth the uncommon definition so as to put one reasonably skilled in the art on notice that the applicant intended to so redefine the claim term." (See Office Action dated June 22, 2007 at page 3). Furthermore, the Examiner alleges "Applicant fails to meet the requirements of redefining a term as set forth in the MPEP § 2106. In order to define/redefine a term, the Applicant must do so "with reasonable clarity, deliberateness, and precision" and must "set out his uncommon definition in some manner within the patent disclosure" so as to give one of ordinary skill in the art notice of the change" in meaning." (See Office Action dated June 22, 2007 at page 4).

Appellants respectfully submit, however, that Appellants are not redefining the term "hash", as alleged by the Examiner. That is, Appellants are using the term hash function as

defined in, for instance, the book “Handbook of Applied Cryptography”, which defines a hash function as a function, which is near-collision resistant. As previously submitted, comparing the hashes by themselves will not work. An important feature of the claimed invention is the addition of other processing steps, which allow comparison of similar processed biometric data and which compare the resulting hashes.

In particular, the function  $h$  in the claims is not a hash function and the language in the claims did not specify that  $h$  is a cryptographic hash function. For instance, in claim 15, the use of a secure hash function is only one part of the algorithm to compute  $h$ .

The Examiner has mistakenly assumed that the  $h(P)$  in the disclosure is equal to the cryptographic hash of the biometric data  $P$ .

To summarize, the Examiner appears to have erroneously summarized the teachings of the present invention in a way which clearly does not comport with the actual disclosure of the invention. Indeed, the present invention clearly is not contrary to the teachings of the Handbook of Applied Cryptography, but instead, acknowledges the very problem identified in the Handbook by the Examiner and provides a novel solution for circumventing such problems.

Thus, the Examiner's assertion that “Applicant failed to provide sufficient evidence to assert the invention's operability, therefore, the 101 rejection stands” clearly is inappropriate, and indeed, is not germane to the rejections since the Examiner has not explained or provided

any reasons as to why the actual disclosure of the present application would be inoperative and lack utility.

For the foregoing reasons, Appellants respectfully submit that a person of ordinary skill in the art to which the invention pertains would recognize the utility of the claimed invention and would know and understand the claimed invention. Thus, the Examiner is requested to reconsider and withdraw this rejection.

**2. REJECTION UNDER 35 U.S.C. § 101 (Alleged Non-Statutory Subject Matter)**

The Examiner alleges that the claimed invention of claims 31-36 is directed to non-statutory subject matter. Specifically, the Examiner alleges “[t]he Office’s current position is that claims involving signals encoded with functional descriptive material do not fall within any of the categories of patentable subject matter set forth in 35 U.S.C. § 101, and such claims are therefore ineligible for patent protection.” (See Office Action dated June 22, 2007 at page 9).

Appellants respectfully submit, however, that claims 31-36 are not directed to and do not recite an electromagnetic signal (as addressed in Annex IV(c) of the Interim Guidelines on Patentability).

That is, claims 31-36 are directed to a “computer-readable medium”. Indeed, M.P.E.P. § 2106 clearly sets forth that computer-related product claims are statutory subject matter. That is, “[i]f a claim defines a useful machine or manufacture by identifying the physical structure or the

Appellants' Brief on Appeal  
U.S. Application Serial No. 09/457,732  
Docket No. YOR919990137US1  
(YOR.080)

machine or manufacture in terms of its hardware or hardware and software combination, it defines a statutory product”.

Along these lines, the Court in *In re Beauregard* upheld a computer program as patentable subject matter because it was claimed in terms of an article of manufacture as contained on a floppy disk (see *In re Beauregard*, 53 F.35 1583 (Fed. Cir. 1995)). Beauregard claims protect computer-related media encoded with a computer program because such media are viewed as computer elements that define structural and functional interrelationships between the computer program and the computer. Thus, Beauregard claims define statutory subject matter as long as the claim language defines a relationship between the encoded program and a computer.

Thus, the Examiner is requested to reconsider and withdraw this rejection.

### **3. THE PRIOR ART REJECTION**

Claims 1, 5-9, and 11-36 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Borza in view of Kharon. Appellants respectfully traverse this rejection, for at least the following reasons.

As mentioned above, the traversal arguments set forth in the Amendment under 37 C.F.R. § 1.111 filed on June 18, 2004, the Amendment under 37 C.F.R. § 1.116 filed on January 18, 2005, the Amendment under 37 C.F.R. § 1.111 filed on April 15, 2005, the Amendment under 37 C.F.R. § 1.116 filed on July 11, 2005, the Amendment under 37

C.F.R. § 1.111 filed on December 16, 2005, the Amendment under 37 C.F.R. § 1.111 filed on January 16, 2007, and the Amendment under 37 C.F.R. § 1.116 filed on August 22, 2007 are incorporated herein by reference in their entirety.

**a) THE CLAIMED INVENTION**

The claimed invention provides a method and system of processing semiotic data that allows use of the data without being a threat to privacy and that prevents misuse of such data, without significantly altering the accuracy and sensitivity of the identification process (e.g., see specification at page 3, lines 9-14).

For example, the claimed invention compares encrypted data against stored encrypted data while at the same time ensuring that unencrypted data is not available or retrievable under the condition that the data might be slightly different from the template. That is, the claimed invention determines whether P is close to P' by comparing only h(P) with h(P'). Thus, in contrast to conventional methods, the claimed invention compares encrypted data against an encrypted template under the possibility that the data might be slightly different from the template (e.g., "close" to the data) (e.g., see specification at page 16, lines 12-17, and pages 17-20).

**b) EXAMINER'S POSITION IS FLAWED AS A MATTER  
OF FACT AND LAW**

Appellants respectfully submit that the Examiner's position is flawed as a matter of fact and law.

First, as Appellants have pointed out, Borza does not expressly anticipate or make obvious all of the elements of the claimed invention. Thus, irrespective of the operability of Borza, Appellants submit that the alleged combination of Borza and Kharon does not disclose or suggest all of the features of the claimed invention.

Instead, Borza only generally mentions that a comparison of encrypted data is done, but does not disclose the specific features recited in the claimed invention. In fact, Borza clearly does not discuss *how* it compares encrypted data.

In fact, the cited portion of Borza at column 16, lines 31-38 does not determine whether  $h(P)$  is close to  $h(P')$ , as alleged by the Examiner. Indeed, it is unclear how Borza at column 16, lines 31-38 even relates to the disclosure of comparing encrypted data against an encrypted template at column 8, lines 28-38.

That is, nowhere at column 16, lines 31-38, or in Figure 13 which is being described therein, does Borza mention comparing encrypted data against an encrypted template. Thus, the Examiner has mischaracterized the teachings of Borza.

Second, even assuming *arguendo* that Borza is operative, the disclosure provided by Borza fails to teach or suggest all of the features of the claimed invention for which it is

being relied upon. Therefore, the alleged combination of Borza and Kharon clearly does not disclose or suggest all of the features of the claimed invention.

In other words, irrespective of the operability of Borza, the disclosure of Borza clearly does not disclose or suggest *how* to compare two encrypted data sets to determine similarity between the two original data sets according to the features recited in the claimed invention.

Appellants reiterate that the ordinarily skilled artisan would understand that encryption causes diffusion of data, which means that the encryption of two similar, but not identical data sets create two encrypted data sets that are very different. Thus, merely comparing two encrypted data sets still would not (and does not) disclose or suggest the similarity between the two unencrypted data sets.

In fact, as the Examiner points out, and as Appellants specifically acknowledge in the specification, no identification is possible by direct comparison of the encrypted data.

Thus, in contrast to Borza, the claimed invention discloses several approaches to compare encrypted or hashed data under such uncertainty (e.g., see specification at page 16, line 18 to page 20, line 8).

Specifically, as mentioned above, the disclosure of the present invention specifically acknowledges the problem that a simple hash function approach would not work (as suggested by the Examiner)(e.g., see specification at page 16, lines 15-17).

For example, the specification of the present application (at page 16, lines 15-17) specifically states that:

Because  $P_0$  is in general (possibly) slightly different from  $P_i$  for  $i > 0$ , the secret version of  $p_0$  will generally be quite different from the secret version of  $P_i$ . This is because cryptographic functions are extremely sensitive to the input, thereby to be resilient to attempts to decode the encrypted data. In this case, no identification is possible by direct comparison of the encrypted data (emphasis added).

Accordingly, the present application discloses several approaches to compare encrypted or hashed data under such uncertainty (e.g., see specification at page 16, line 18 to page 20, line 8).

That is, the specification specifically describes three basis methods to circumvent this situation and the sensitivity of the cryptographic functions (e.g., see specification at page 16, lines 18-19). Indeed, pages 17-20 of the specification specifically describe first, second, and third methods for circumventing the very problem with comparing encrypted or hash data which the Examiner mentions.

The claimed invention compares encrypted data against stored encrypted data while at the same time ensuring that unencrypted data is not available or retrievable under the condition that the data might be slightly different from the template. That is, the claimed invention determines whether P is close to P' by comparing only h(P) with h(P') (e.g., see specification at page 16, lines 12-17, and pages 17-20).



The present application explains that, in contrast to conventional methods, the claimed invention compares encrypted data against an encrypted template under the possibility that the data might be slightly different from the template (e.g., “close” to the data) (e.g., see specification at page 16, lines 12-17, and pages 17-20).

Thus, the claimed invention solves the problem that a simple hash function approach would not work (as suggested by the Examiner in the Office Action at page 4, numbered paragraph 11)(e.g., see specification at page 16, lines 15-17) by circumventing the problem, as disclosed and claimed.

For the foregoing reasons, Borza clearly does not disclose or suggest at least “*to determine whether  $P'$  is close to a predetermined subject, comparing  $h(P')$  to available  $h(P)$ s to determine whether  $P'$  substantially matches, but does not exactly match, one of said data set  $P'$* ”, as recited in claim 1.

Independent claims 5, 9, 15, 17, 19, 24, 27, 29, 31, 33, and 35 recite somewhat similar features. Therefore, Appellants submit that Independent claims 5, 9, 15, 17, 19, 24, 27, 29, 31, 33, and 35 also are patentable over the prior art of record for the same reasons as independent claim 1.

On the other hand, Appellants respectfully reiterate that Kharon does not make up for the deficiencies of Borza.

The Examiner relies on Kharon for teaching the claimed “extracting sub-collections  $S_j$  from the collection of data in data set  $P$ ; encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability, comparing encrypted versions of the sub-collections  $S_j$  with those data stored in said database, wherein if one or more of the sub-collection  $S_j$  matches with said data, then verification is deemed to have occurred”, as recited in independent claim 1.

However, contrary to the Examiner’s position, Kharon (at column 13, lines 43-67) does not describe extracting multiple subsets  $S_j$  (i.e., “sub-collections”) from the data. Furthermore, Kharon does not describe encrypting a number of such subsets (i.e., a “number of such sub-collections”) such that at least one is reproduced exactly with a predetermined probability.

Appellants respectfully submit that the Examiner seems to have confused using a smaller section of the data for verification (which would be less desirable since less data is used), whereas the claimed invention uses multiple subsets of the data for verification.

Thus, using just a smaller subset of the data for verification would be less desirable since it is easy to forge the data and does not solve the problem of being able to compare two encrypted data.

On the other hand, using multiple subsets of the data, according to the claimed invention, allows encrypted data to be compared and to generate a measure of similarity.

Moreover, In the Examiner's Answer dated November 13, 2006, the Examiner states that:

In response to appellant's argument that the claimed invention provides a method and system for processing semiotic data that allows use of the data without being a threat to privacy and that prevents misuse of such data, without significantly altering the accuracy and sensitivity of the identification process, a recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claim.

(see Examiner's Answer at page 15).

Appellants respectfully submit, however, that independent claim 1 defines a "method", and therefore, it is unclear how the Examiner's statement is germane to independent claim 1.

In the Examiner's Answer dated November 13, 2006, the Examiner states that:

In response to appellant's argument that the references fail to show certain features of appellant's invention, it is noted that the features, such as how the comparison between the two data sets are compared, upon which appellant relies are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). The Appellant does not claim the structure that does the comparing between the two encrypted samples, but instead claims the method steps which the Examiner has shown to be taught by *Borza*.

(see Examiner's Answer at page 15).

Appellants respectfully submit, however, that independent claims 24 and 29 recite “system” claims. Therefore, it is unclear how the Examiner’s statement is germane to independent claims 24 and 29.

In the Examiner’s Answer dated November 13, 2006, the Examiner further states that:

In response to the Appellant’s arguments that *Borza* does not determine whether  $h(P)$  is close to  $h(P')$ , the Examiner disagrees. *Borza* discloses at column 16, lines 19-38 discloses techniques for determining the identification of someone by acquiring a biometric sample and comparing it to the stored templates. If the sample acquired for authentication is within predetermined range of the template, identification is provided for, if it is outside that predetermined range, then the user is not authenticated. *Borza* teaches comparing encrypted samples to encrypted templates in column 8, lines 28-38. The Appellant is reminded of MPEP 2123, which states that patents are relevant as prior art for all they contain.

(see Examiner’s Answer at page 15).

The Examiner further states that “*Borza* discloses determining whether  $h(P)$  is close to  $h(P')$ , without having to be identical matches, when comparing encrypted samples to encrypted templates, and the rejection should be maintained.” (see Examiner’s Answer at page 15).

Appellants respectfully disagree.

First, *Borza* discloses that “[w]hen a substantial match occurs between a template and the characterized biometric information” (see *Borza* at column 8, lines 9-12). The characterized biometric information is not, however, encrypted information.

On the other hand, column 8, lines 28-30 describe comparing the encrypted characterized biometric information to against an encrypted template. However, Borza fails to describe how the encrypted information could be compared to determine a substantial match, and indeed, does not state that a substantial match is determined, when Borza describes the encrypted information.

Thus, contrary to the Examiner's position, Borza does not disclose the features for which it is being relied upon.

The Examiner further states that:

In response to the Appellant's argument that *Kharon* does not disclose extracting multiple subsets of data, the Examiner states that, "In column 14, lines 40-53 *Kharon* discloses the k`" minutia and groupings of minutia. *Kharon* also states at column 13, lines 63-67 that the data set is defined so that N represents the total number of minutia for the fingerprint. *Kharon* discloses extracting multiple subsets from the data in disclosing multiple instances of the minutia, and the rejection should be upheld."

(see Examiner's Answer at page 15).

In response to the Appellant's argument that *Kharon* does not teaches comparing encrypted versions of the sub-collection with those stored in the database, the Examiner disagrees.

The Examiner states that "As shown above, *Borza* provides a showing of comparing two encrypted data sets for authentication purposes. *Kharon* teaches at column 14, lines 1-9 of comparing the minutia data sets to that of a database for authenticating the fingerprint.

Therefore, the combination of references discloses comparing encrypted subsets of data against a database for verification and the rejection should be maintained.” (see Examiner’s Answer at pages 16-17).

Appellants respectfully disagree.

First, the Examiner seems to agree with Appellants that Kharon does not teach comparing encrypted versions of the sub-collection with those stored in the database. Instead, Kharon teaches only comparing unencrypted data. That is, the Examiner now takes the position that the combination of Borza and Kharon teach this feature.

Second, assuming *arguendo* that, as the Examiner asserts, Borza provides a showing of comparing two encrypted data sets for authentication purposes, and that Kharon teaches at comparing the minutia data sets to that of a database for authenticating a fingerprint, Applicants submit that the ordinarily skilled artisan would not have been motivated to combine these features to arrive at the claimed invention, for at least the following reasons.

First, Applicants respectfully submit that the Examiner has not provided sufficient reasoning for combining these references.

That is, the Examiner alleges that “It would have been obvious to one of ordinary skill in the art at the time the invention was made to sample a smaller section of the data set. One would be motivated to do because there is a better probability that a smaller area is less likely

to change, therefore making it more difficult for someone to steal someone's identification”  
(see Examiner's Answer at page 7).

However, the Examiner does not provide, or cite, any support for the alleged reason to combine these references. Indeed, it is unclear whether one or more of the references are deemed to provide an reasoning, or if the Examiner is relying on the general knowledge within the art for such reasoning.

Thus, as a procedural matter, and as a matter of law, the Examiner has not established a *prima facie* case of obviousness.

Appellants note that, "In determining the propriety of the Patent Office case for obviousness in the first instance, it is necessary to ascertain whether or not the reference teachings would appear to be sufficient for one of ordinary skill in the relevant art having the reference before him to make the proposed substitution, combination, or other modification." In re Linter, 458 F.2d 1013, 1016, 173 USPQ 560, 562 (CCPA 1972)" (citing M.P.E.P. § 2143.01).

Moreover, notwithstanding the above, Appellants respectfully submit that it would not have been obvious to combine these references in the manner alleged, since neither Borza nor Kharon provide any teaching of how such a combination would be made.

It is noted that, although a prior art device "may be capable of being modified to run the way the apparatus is claimed, there must be a suggestion or motivation in the reference to

do so." 916 F.2d at 682, 16 USPQ2d at 1432.). See also In re Fritch, 972 F.2d 1260, 23 USPQ2d 1780 (Fed. Cir. 1992) (flexible landscape edging device which is conformable to a ground surface of varying slope not suggested by combination of prior art references).

That is, it is not enough merely to combine the teachings of the references based on the teachings of Appellants's invention (i.e., impermissible hindsight based analysis).

Instead, the Examiner must show that there would have been a reasons for an ordinarily skilled artisan, having read the teachings of Borza and Kharon, would, by the references themselves, or the teachings of art in general, to make the claimed combination.

Thus, as a matter of law, the Examiner has not established a *prima facie* case of obviousness.

Moreover, in the Examiner's Response to Arguments included in the Office Action dated June 22, 2007, the Examiner alleges, "*Borza* discloses determining whether  $h(P)$  is close to  $h(P')$ , without having to be identical matches, when comparing encrypted samples to encrypted templates, and the rejection should be maintained." (See Office Action dated June 22, 2007 at page 5). The Examiner, however, is clearly incorrect.

That is, Borza merely discloses comparing biometric data  $P$ , not the privacy protected version of the biometric data  $h(P)$ , which is recited in the claimed invention (e.g., see Borza at column 16, lines 19-37 and Figure 13). Borza does not compare encrypted biometric data. For



example, in column 6, lines 19-21 of Borza, the encrypted data is first decrypted before comparison, so in fact the unencrypted biometric data is compared.

Furthermore, the Examiner alleges, "extracting subsets of data and comparing encrypted subsets of data, are not recited in all of the rejected independent claims." (See Office Action dated June 22, 2007 at page 7). Appellants respectfully submit, however, that these features are recited in at least dependent claim 17 and Appellants comments are therefore relevant to the claimed invention.

Thus, for the foregoing reasons, Appellants respectfully submit that Borza and Kharon, either individually or in combination, discloses or suggests all of the features of the claimed invention. Therefore, the Examiner is requested to reconsider and withdraw this rejection.

In view of all of the foregoing, Appellants submit that all of the pending claims (i.e., claims 1 and 5-36) are patentable over the prior art of record.

## **VIII. CONCLUSION**

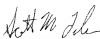
In view of the foregoing, Appellants submit that Claims 1 and 5-36 of the application are patentably distinct from the prior art of record and in condition for allowance. Thus, the Board is respectfully requested to remove the rejections of Claims 1 and 5-36.

Appellants' Brief on Appeal  
U.S. Application Serial No. 09/457,732  
Docket No. YOR919990137US1  
(YOR.080)

Please charge any deficiencies and/or credit any overpayments necessary to enter this paper to Assignee's Deposit Account No. 50-0510.

Respectfully Submitted,

Date: November 26, 2007



\_\_\_\_\_  
Scott M. Tulino, Esq.  
Registration No. 48,317

Sean M. McGinn, Esq.  
Registration No. 34,386

**MCGINN INTELLECTUAL PROPERTY  
LAW GROUP, PLLC**  
8321 Old Courthouse Road, Suite 200  
Vienna, Virginia 22182-3817  
(703) 761-4100  
**Customer No. 48150**

**CLAIMS APPENDIX**

1. A method of processing semiotic data, comprising:
  - receiving semiotic data including at least one data set P,
  - selecting a function h, and for at least one of each said data set P to be collected,
  - computing h(P);
  - destroying said data set P,
  - storing h(P) in a database, and
  - obtaining a sample of P' such that a comparison can be made;
  - at least one of obtaining and computing h(P'); and
  - to determine whether P' is close to a predetermined subject, comparing h(P') to available h(P)s to determine whether P' substantially matches, but does not exactly match, one of said data set P,
  - wherein said data set P cannot be extracted from h(P),
  - wherein said semiotic data comprises biometric data,
  - wherein said function h comprises a secure hash function,
  - wherein the data set P is not determined perfectly by its reading,

wherein each reading gives a number  $P_i$ , wherein  $i$  is no less than 0, wherein  $P_0$  is for an initial reading, and a secret version of said initial reading is stored after further processing thereof,

wherein reading  $P_0$  is different from  $P_i$  for  $i > 0$ , and the secret version of  $P_0$  is different from the secret version of  $P_i$ , such that no identification is possible by a direct comparison of the encrypted data,

said method further comprising:

extracting sub-collections  $S_j$  from the collection of data in data set  $P$ ,

encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability,

comparing encrypted versions of the sub-collections  $S_j$  with those data stored in said database,

wherein if one or more of the sub-collection  $S_j$  matches with said data, then verification is deemed to have occurred,

each time a  $P_i$ , with  $i > 0$ , is read, computing all possible predetermined size variations of  $P_i$  which correspond to an acceptable predetermined imprecision of the reading; and

encrypting all such modified data, and comparing said encrypted modified data to data stored in said database,

wherein for a plurality of users of the same biometric information, said biometric information is encrypted differently for each user, and

wherein at least one of said data set P and P' comprises a personal data set.

5. A method of processing semiotic data, comprising:
  - receiving semiotic data including at least one data set P;
  - selecting a function h, and for at least one of each said data set P to be collected, computing h(P);
  - destroying said data set P, and
  - storing h(P) in a database,
  - wherein said data set P cannot be extracted from h(P),
  - the method further comprising:
    - selecting a private key/public key (K, k) once for all cases; and
    - one of destroying said private key K and sending said private key K to a trusted party;
  - and
  - choosing said function h as the public encryption function corresponding to k.
6. The method according to claim 5, wherein said data set P cannot be extracted from h(P), except by the trusted party.

7. The method according to claim 5, further comprising:  
  
to determine whether some  $P'$  is a predetermined subject, comparing said  $h(P')$  to available  $h(P)$ s; and  
  
determining whether there is a match.
  
8. The method according to claim 5, wherein the trusted party comprises a panel of members, and  
  
wherein a secret is shared among the members so that only at least a predetermined number of panel members can reconstitute the secret in its entirety by putting together their share of the secret.
  
9. A method of processing semiotic data, comprising:  
  
receiving semiotic data including at least one data set  $P$ ;  
  
selecting a function  $h$ , and for at least one of each said data set  $P$  to be collected,  
  
computing  $h(P)$ ;  
  
destroying said data set  $P$ ;  
  
storing  $h(P)$  in a database,  
  
wherein said data set  $P$  cannot be extracted from  $h(P)$ ,

wherein the data set  $P$  is not determined perfectly by its reading,

wherein each reading gives a number  $P_i$ , wherein  $i$  is no less than 0, wherein  $P_0$  is for an initial reading, and a secret version of said initial reading is stored after further processing thereof,

wherein reading  $P_0$  is different from  $P_i$  for  $i > 0$ , and the secret version of  $P_0$  is different from the secret version of  $P_i$ , such that no identification is possible by a direct comparison of the encrypted data;

extracting sub-collections  $S_j$  from the collection of data in data set  $P$ ; and

encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability.

11. The method according to claim 9, further comprising:

comparing encrypted versions of the sub-collections  $S_j$  with those data stored in said database,

wherein if one or more of the sub-collection  $S_j$  matches with said data, then verification is deemed to have occurred.

12. The method according to claim 11, further comprising:

each time a  $P_i$ , with  $i > 0$ , is read, computing all possible predetermined size variations of  $P_i$  which correspond to an acceptable predetermined imprecision of the reading; and

encrypting all such modified data, and comparing said encrypted modified data to data stored in said database.

13. The method according to claim 12, wherein for a plurality of users of the same biometric information, said biometric information is encrypted differently for each user.

14. The method according to claim 1, wherein at least one of said data set  $P$  and  $P'$  comprises a personal data set.

15. A method of processing biometric data, comprising:  
acquiring unencrypted biometric data including at least one data set  $P$ ;  
encrypting, with one of a secure hash function and an identity function, each said at least one data set acquired;  
destroying the unencrypted data set  $P$ ;  
storing each of the at least one encrypted data set in a database,



wherein unencrypted biometric data is not available nor retrievable from said data stored in said database, and

to determine whether a data set P' is a predetermined subject, comparing an encrypted data set of P' to the at least one encrypted data set stored in the database to determine whether the data set P' substantially matches, but does not exactly match, the at least one encrypted data set stored in the database,

said method further comprising:

extracting sub-collections S<sub>j</sub> from the collection of data in data set P;

encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability,

comparing encrypted versions of the sub-collections S<sub>j</sub> with those data stored in said database,

wherein if one or more of the sub-collection S<sub>j</sub> matches with said data, then verification is deemed to have occurred.

16. The method according to claim 15, wherein at least one of said data set P and P' comprises a personal data set.

17. A method of extracting components of biometric data which are stable under measurement errors, comprising:

acquiring unencrypted biometric data including at least one data set P;  
encrypting each said at least one data set acquired to form at least one encrypted data set;

destroying the unencrypted data set P;  
storing each said at least one encrypted data set in a database,  
wherein unencrypted biometric data is not available nor retrievable from said data stored in said database, and

to determine whether a data set P' is a predetermined subject, comparing an encrypted data set of P' to the at least one encrypted data set stored in the database to determine whether there is a match,

said method further comprising:

extracting sub-collections S<sub>j</sub> from the collection of data in data set P;  
encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability,  
comparing encrypted versions of the sub-collections S<sub>j</sub> with those data stored in said database,

wherein if one or more of the sub-collection  $S_j$  matches with said data, then verification is deemed to have occurred.

18. The method according to claim 17, wherein at least one of said data set P and P' comprises a personal data set.

19. A method of extracting components of biometric data which are stable under measurement errors, comprising:

acquiring unencrypted biometric data including at least one data set P;  
encrypting each said at least one data set acquired to form at least one encrypted data set;

destroying the unencrypted data set P; and  
storing each said at least one encrypted data set in a database,  
wherein unencrypted biometric data is not available nor retrievable from said data stored in said database,

extracting sub-collections  $S_j$  from the collection of data in said data set P; and  
encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability.

20. The method according to claim 19, wherein said data set comprises a personal data set.
21. The method according to claim 19, further comprising:  
comparing encrypted versions of the sub-collections  $S_j$  with those data stored in said database,  
wherein if one or more of the sub-collection  $S_j$  matches with said data, then verification is deemed to have occurred.
22. The method according to claim 21, wherein a data set  $P$  is not determined perfectly by its reading, such that each reading gives a number  $P_i$ ,  
wherein  $i$  is no less than 0,  
wherein  $P_0$  is for an initial reading, and a secret version of said initial reading is stored after further processing thereof,  
wherein reading  $P_0$  is different from  $P_i$  for  $i > 0$ , and the secret version of  $P_0$  is different from the secret version of  $P_i$ , such that no identification is possible by a direct comparison of the encrypted data.
23. The method according to claim 21, further comprising:

each time a data set is read  $P_i$ , with  $i > 0$ , is read, computing all possible predetermined size variations of  $P_i$  which correspond to an acceptable predetermined imprecision of the reading; and

encrypting all such modified data, and comparing said encrypted modified data to data stored in said database.

24. A system for processing semiotic data, comprising:

means for receiving semiotic data including a data set  $P$ ;

means for selecting a function  $h$ , and for each said data set  $P$  to be collected, computing  $h(P)$ ;

means for destroying said data set  $P$ ;

means for storing  $h(P)$  in a database, wherein said data set  $P$  cannot be extracted from  $h(P)$ , and

to determine whether a data set  $P'$  is close to a predetermined subject, means for comparing  $h(P')$  to available  $h(P)$ s to determine whether data set  $P'$  is close to some  $P$ .

25. A system of processing semiotic data as in claim 24, wherein said semiotic data comprises biometric data.

26. The system according to claim 24, wherein at least one of said data set P and P' comprises a personal data set.

27. A system for verifying biometric data without storing unencrypted biometric data, comprising:

means for acquiring unencrypted biometric data including at least one data set P;

means for encrypting each said at least one data set acquired to form at least one encrypted data set; means for destroying the unencrypted data set P;

means for storing each said at least one encrypted data set in a database, wherein unencrypted biometric data is not available nor retrievable from said data stored in said database, and

means for comparing an encrypted data set of a data set P' to said at least one encrypted data set of data set P to determine whether there is a match and to determine whether the data set P' is a predetermined subject.

28. The system according to claim 27, wherein at least one of said data set P and P' comprises a personal data set.

29. A system for extracting components of biometric data which are stable under measurement errors, comprising:

acquiring unencrypted biometric data including at least one data set P; encrypting each said at least one data set acquired to form at least one encrypted data set;

destroying the unencrypted data set P; and

storing each said at least one encrypted data set in a database,

wherein unencrypted biometric data is not available nor retrievable from said data stored in said database,

extracting sub-collections  $S_j$  from the collection of data in said data set P; and

encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability.

30. The system according to claim 29, wherein said data set comprises a personal data set.

31. A computer-readable medium tangibly embodying a program of recordable, machine-readable instructions executable by a digital processing apparatus to perform a method for computer-implemented processing biometric data, said method comprising:

receiving biometric data including a data set P;

selecting a secure hash function  $h$ , and for each data set  $P$  to be collected, computing  $h(P)$ ;  
destroying said data set  $P$ ;  
storing  $h(P)$  in a database, wherein said data set  $P$  cannot be extracted from  $h(P)$ , and  
to determine whether a data set  $P'$  is close to a predetermined subject, comparing  $h(P')$   
to available  $h(P)$ s to determine whether data set  $P'$  is close to some data set  $P$ .

32. The computer-readable medium according to claim 31, wherein at least one of said data set  $P$  and  $P'$  comprises a personal data set.

33. A computer-readable medium tangibly embodying a program of machine-readable instructions executable by a digital processing apparatus to perform a method for computer-implemented verifying of biometric data without storing unencrypted biometric data, said method comprising:

acquiring unencrypted biometric data including at least one data set  $P$ ;  
encrypting each said at least one data set acquired to form at least one encrypted data set;  
destroying the unencrypted data set  $P$ ;



storing each said at least one encrypted data set in a database, wherein unencrypted biometric data is not available nor retrievable from said data stored in said database, and

to determine whether a data set P' is close to a predetermined subject, comparing an encrypted data set of P' to said at least one encrypted data set to determine whether data set P' is close to some data set P,

said method further comprising:

extracting sub-collections S<sub>j</sub> from the collection of data in data set P;

encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability,

comparing encrypted versions of the sub-collections S<sub>j</sub> with those data stored in said database,

wherein if one or more of the sub-collection S<sub>j</sub> matches with said data, then verification is deemed to have occurred.

34. The computer-readable medium according to claim 33, wherein at least one of said data set P and P' comprises a personal data set.

35. A computer-readable medium tangibly embodying a program of recordable, machine-readable instructions executable by a digital processing apparatus to perform a method for

computer-implemented extracting components of biometric data which are stable under measurement errors, said method comprising:

acquiring unencrypted biometric data including at least one data set P; encrypting each said at least one data set acquired to form at least one encrypted data set;

destroying the unencrypted data set P;

storing each said at least one encrypted data set in a database, wherein unencrypted biometric data is not available nor retrievable from said data stored in said database;

extracting sub-collections  $S_j$  from the collection of data in said data set P; and

encrypting a predetermined number of such sub-collections such that at least one of the sub-collections is reproduced exactly with a predetermined probability.

36. The computer-readable medium according to claim 35, wherein said data set comprises a personal data set.

Appellants' Brief on Appeal  
U.S. Application Serial No. 09/457,732  
Docket No. YOR919990137US1  
(YOR.080)

**EVIDENCE APPENDIX**

Not applicable.

Docket No. YOR919990137US1  
YOR.080

**RELATED PROCEEDINGS APPENDIX**

Not applicable.